

MOTHERBOARD
TECH BY VICE

OPM Hackers Used Marvel Superhero Nicknames to Hide Their Tracks

Chinese hackers have a trolly sense of humor.

By [Lorenzo Franceschi-Bicchieri](#)

September 7, 2016, 3:00pm [Share](#) [Tweet](#) [Snap](#)



IMAGE: [ANDY ROTH](#)/FLICKR

The disastrous [data breach](#) discovered last year at the US government agency that handles all federal employees data, the Office of Personnel Management, or [OPM](#), was enabled by a seemingly endless series of mistakes by the agency itself, according to a comprehensive [congressional report](#) released on Wednesday.

The hack, which resulted in the loss of the sensitive personal records of [21.5 million government employees](#), including [5.6 million of their fingerprints](#), was carried out by two hacking groups, likely from China and affiliated with the Chinese government. The hackers took advantage of OPM's lax security and failure to implement "basic cyber hygiene," the report states.

Read more: [FBI Says a Mysterious Hacking Group Has Had Access to US Govt Files for Years](#)

The hackers not only embarrassed OPM by breaching it and going undetected for months, they also trolled the agency's forensic investigators, using Marvel superhero names to steal the data under their noses, the report revealed.

In March of 2014, OPM found about about the hack, which actually started in July of 2012, according to the report's timeline. At that point, with the help of the U.S. Department of Homeland Security's Computer Emergency Readiness Team (US-CERT), which alerted OPM of the breach, the agency started monitoring the hackers' activities.

In an attempt to kick out Captain America, OPM failed to see that Iron Man was also inside their networks

A month later, the hackers registered the domain "Opmsecurity[.]org" under the name of Steve Rogers, Captain America's alter ego. This is one of the domains that the hackers would later use as a command and control server to steal OPM's data.

At that point, OPM thought it had the hackers' under control, but while they were monitoring the first hacker group, another one broke in, posing as an employee of an OPM contractor in May of 2014. Then OPM tried to kick out the first hackers in an operation they nicknamed "Big Bang." The clean-up was deemed a success, according to the report, which was commissioned by the U.S. House Oversight & Government Reform Committee.

However, the second hacker or hackers were actually still inside. And at the end of July of 2014, they registered another domain "opmlerning[.]org" under the name of Tony Stark, also known as Iron Man. The hackers would later use this domain as a command and control server and to get data out of OPM, the report stated.

To sum it up, in an attempt to kick out Captain America, OPM failed to see that Iron Man was also inside their networks, ready to steal a crapload of sensitive data on American government workers. This could be the plot of a slightly ridiculous Avengers sequel, but in this case, it was real, and Captain America and Iron Man were allegedly Chinese government hackers.

Good trolling, Chinese hackers.

Want more Motherboard in your life? Then [sign up for our daily newsletter](#).

TAGGED: [TECH](#), [MOTHERBOARD](#), [HACKING](#), [MARVEL](#), [HACKERS](#), [OPM HACK](#), [IRON MAN](#), [OPM](#), [CAPTAIN AMERICA](#), [MOTHERBOARD SHOW](#), [INTERNET INSECURITY](#)

GET A PERSONALIZED ROUNDUP OF VICE'S BEST STORIES IN YOUR INBOX.

Subscribe

By signing up to the VICE newsletter you agree to receive electronic communications from VICE that may sometimes include advertisements or sponsored content.